REMARKS

Reconsideration and withdrawal of the rejections set forth in the Office Action dated June 12, 2003, are respectfully requested. A separate petition for a three-month extension of time accompanies this amendment.

As an initial matter, the applicant wishes to bring the Examiner's attention to two supplemental information disclosure statements that were mailed May 15, 2001 and June 26, 2003, which have not been acknowledged by the Examiner. For the Examiner's convenience, duplicate copies of these supplemental information disclosure statements are enclosed with this response, both of which bear first class mailing certificates, together with copies of returned postcards received from the Patent Office.

I. Disclosed Embodiments of the Invention

Conventional voting schemes employ a two step process. First, the voter registers, which typically involves the voter submitting his or her signature to a registrar. Second, the voter signs in at a poll, or signs an envelope enclosing a ballot, which allows the voter's signature to later be compared to the earlier provided signature held by the registrant. Under the second step, systems are provided to keep the voter's identity confidential with respect to his or her ballot, and ensure that ballots are not compromised.

Published articles and other references address have discussed how to provide electronic voting that ensures the privacy of each voter, as well as provide security to prevent voting fraud. Such references address ensuring the privacy of voters, such as through encryption, as well as authentication schemes to ensure that electronic ballots have not been tampered with. Such references, however, address only the second step in a voting process -- they fail to address registering voters.

Embodiments of the invention address such registration, namely the first step employed in conventional voting schemes. For example, one embodiment describes a method of how each eligible registrant obtains a public/private key pair that meets pre-defined format and security specifications of the registrar, authenticating authority, or

both. A public key of each eligible registrant is distributed to an organization administering the registration (a registrar), and the registrar maintains a record of each eligible registrant's public key. The disclosed embodiment protects the registrar from accepting and recording public keys from perspective registrants where the public keys have been generated by some illegitimate source, from non-existent individuals, or are to be used for some illegitimate reasons. Thus, embodiments are directed to registration processes so that the registrar can properly identify prospective registrants and record the public key of each prospective voter registrant.

I.   Rejections under 35 U.S.C. §102

The Examiner rejected all claims 1-40 as unpatentable under 35 U.S.C. §102(e) as anticipated by a thesis by M. Herschberg entitled "Secure Electronic Voting over the Worldwide Web." (Attorneys for the applicant believe that the rejection should be under 102 (b), because the applied reference is not a US Patent or application.) As explained below, the applicant respectively submits that Herschberg fails to disclose or fairly suggest the applicant's claimed invention.

A.   The Applied Art

Herschberg is directed to an electronic voting method conducted over the Internet, which employs known cryptographic processes, such as Blowfish (a block cipher) to encrypt communications, and standard public-private key generating software, such as RSA. Importantly, Herschberg, like the rest of the art, ignores how voters are registered. For example, at Section 6.4.2 entitled "Registration," Herschberg simply says the following:

> The Registrar can create ghosts. That is, it can register non-existent voters and later cast votes under those names. The prevention of ghosts is a policy issue, and <u>not one for cryptography</u>. A practical solution is to have adversarial parties oversee the registration process, to make sure the dead do not rise to vote again. (emphasis added)

As can be seen from the above portion from Herschberg, Herschberg ignores registration as a cryptographic problem, and instead simply says that it is a policy

decision. Similarly in Section 3.2.1 entitled "Authentication," Herschberg notes the following:

> The two options considered for vote identification are a public key system, suggested by the use of digital signatures in Fujioka et al., and a password system. The former was discarded for two reasons. . . . Second, either a public key system must already be in place, or the keys must be distributed in a secure manner. The most likely form of distribution would be for voters [to] get their keys during registration, which requires that they either remember the unwieldy number, or have some sort of secure electronic transfer available.

The above two sections in Herschberg appear to be the most relevant where Herschberg would discuss registration. However, neither of these sections address schemes for voter registration. Indeed, Herschberg simply ignores registration, and instead focuses on the process of handling encrypted ballots after registration.

B.   Analysis

Distinctions between claim 1 and Herschberg will first be discussed, followed by distinctions between Herschberg and the remaining independent claims.[1]

As noted above, Herschberg is directed to employing cryptographic techniques in creating and casting a ballot. He ignores an important first part of any voting scheme, let alone an electronic voting scheme, namely registration. Instead, Herschberg simply says that "the prevention of ghosts is a policy issue."

Thus, Herschberg fails to disclose any method of registration, which is the point of claim 1. Herschberg further fails to disclose any method of registration that employs, for example, written signatures, such as written signatures from each of multiple registrants. Furthermore, Herschberg fails to disclose two channels of communication, one of which includes hand-delivery. Moreover, Herschberg fails to disclose the registration process of handling public keys via two channels of communication, one of which includes hand-delivery.

---

[1] Silence regarding the position taken, or argument made, by the Examiner does not indicate any acquiescence to that position or argument.

In a way, Herschberg teaches away from the claimed invention, because Herschberg ignores registration. Herschberg would instruct one of ordinary skill in the relevant art to ignore registration as a process unrelated to cryptography, and instead push it to public policy officials. The inventor disagrees. Registration instead is an element of electronic voting that should be included in any electronic voting process, as recited in the claimed invention.

As is known, to anticipate a claim under 35 U.S.C. §102, the reference must teach every element of the claim.[2] Herschberg fails to disclose every limitation recited in claim 1. Thus, for at least these reasons, claim 1 is patentable over Herschberg.

The remaining independent claims are allowable for similar reasons. As with claim 1, claims 15, 21, 34-37 and 40 are directed to methods of voter registration. Similarly, claims 11, 17 and 29 are directed to a computer-readable medium whose contents cause a computer to register registrants, while claims 13 and 33 are directed to registration computer systems. Each of these claims includes at least some of the limitations found in claim 1. Thus, for similar reasons, the remaining independent claims 11, 13, 15, 17, 19, 21, 29, 33-37 and 40 are allowable over Herschberg.
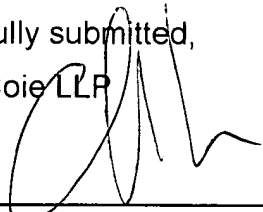
II.   Conclusion

Overall, Herschberg fails to teach or suggest the features recited in independent claims 1, 11, 13, 15, 17, 19, 21, 29, 33-37 and 40, and thus such claims are allowable. Since these independent claims are allowable, based on at least the above reasons, the claims which depend from them are likewise allowable. If the undersigned attorney

---

[2] MPEP section 2131, p. 70 (Feb. 2003, Rev. 1). *See also, Ex parte Levy,* 17 U.S.P.Q.2d 1461, 1462 (Bd. Pat. App. & Interf. 1990) (to establish a *prima facie* case of anticipation, the Examiner must identify where "each and every facet of the claimed invention is disclosed in the applied reference."); *Glaverbel Société Anonyme v. Northlake Mktg. & Supply, Inc.,* 45 F.3d 1550, 1554 (Fed. Cir. 1995) (anticipation requires that each claim element must be identical to a corresponding element in the applied reference); *Atlas Powder Co. v. E.I. duPont De Nemours,* 750 F.2d 1569, 1574 (1984) (the failure to mention "a claimed element (in) a prior art reference is enough to negate anticipation by that reference").

has overlooked a relevant teaching in any of the references, the Examiner is requested to point out specifically where such teaching may be found.

In view of the foregoing, the claims pending in the application comply with the requirements of 35 U.S.C. § 112 and patentably define over the applied art. A Notice of Allowance is, therefore, respectfully requested. If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-3599.

Respectfully submitted,
Perkins Coie LLP

Christopher J. Daley-Watson
Registration No. 34,807

Correspondence Address:
Customer No. 25096
Perkins Coie LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 583-8888